CLAIMS

What is claimed is:

1. An apparatus comprising:

a first key section to be initialized with either a first cipher key, and to successively transform the first cipher key or a selectively modified version of the first cipher key;

a data section coupled to the first key section to be initialized with either a block of plain text or a random number, and to successively and dependently, on the first key section, transform the plain text/random number;

a second key section coupled to the first key section selectively enableable to selectively modify the first cipher key; and

a mapping section coupled to the first key section and the data section to generate a pseudo random bit sequence when the first key section and the data section are initialized with the first cipher key and the random number respectively, and the second key section is selectably enabled to modify the stored first cipher key.

2. The apparatus of claim 1, wherein the first key section comprises a first, a second and a third register to be collectively initialized to said first cipher key.

3. The apparatus of claim 2, wherein the first key section further comprises a plurality of substitution units coupled to the first and the third register to receive the stored content of the first register, make at least partial substitution to the received

content and store the at least partially substituted content into the third register during a round of operation.

4. The apparatus of claim 2, wherein the first key section further comprises a linear transformation unit coupling the second register to the first register to store a linearly transformed version of the content of the second register into the first register during a round of operation.

5. The apparatus of claim 2, wherein the first key section further comprises a linear transformation unit coupling the third register to the second register to store a linearly transformed version of the content of the third register into the second register during a round of operation.

6. The apparatus of claim 1, wherein the data section comprises a first, a second and a third register to be collectively initialized to either the block of plain text or the random number.

7. The apparatus of claim 6, wherein the data section further comprises a plurality of substitution units coupled to the first and the third register to receive the stored content of the first register, make at least partial substitution to the received content and store the at least partially substituted content into the third register during a round of operation.

8. The apparatus of claim 6, wherein the data section further comprises a linear transformation unit coupling the second register to the first register to store a linearly transformed version of the content of the second register into the first register,

factoring into consideration inputs from the first key section, during a round of operation.

9. The apparatus of claim 6, wherein the data section further comprises a linear transformation unit coupling the third register to the second register to store a linearly transformed version of the content of the third register into the second register, factoring into consideration inputs from the first key section, during a round of operation.

10. The apparatus of claim 1, wherein the second key section comprises one or more linear feedback shift registers (LFSRs) to output a first, second and third plurality of data bits; and a combiner function coupled to the LFSRS, and having a network of shuffle units serially coupled to each other, to combine the third plurality of data bits, using the first and second plurality of data bits.

11. The apparatus of claim 1, wherein the mapping section comprises a plurality of logical gates coupled to a first and a second register in said first key and data sections respectively to generate said pseudo random bit sequence.

12. An apparatus comprising:

a key section having a first, a second and a third register to be collectively initialized with a first cipher key, and a first plurality of transformation units coupled to the at least first, second and third registers to successively transform the first cipher key; and

a data section having a fourth, a fifth and a sixth register to be collectively initialized with a block of plain text, and a second plurality of transformation units

coupled to the second, fourth, fifth and sixth registers to successively and dependently, on the key section, transform the plain text.

13. The apparatus of claim 12, wherein the first plurality of transformation units comprise a plurality of substitution units coupled to the first and the third register to receive the stored content of the first register, make at least partial substitution to the received content and store the at least partially substituted content into the third register during a round of operation.

14. The apparatus of claim 12, wherein the first plurality of transformation units comprise a linear transformation unit coupling the second register to the first register to store a linearly transformed version of the content of the second register into the first register during a round of operation.

15. The apparatus of claim 12, wherein the first plurality of transformation units comprise a linear transformation unit coupling the third register to the second register to store a linearly transformed version of the content of the third register into the second register during a round of operation.

16. The apparatus of claim 12, wherein the second plurality of transformation units comprise a plurality of substitution units coupled to the fourth and the sixth register to receive the stored content of the fourth register, make at least partial substitution to the received content and store the at least partially substituted content into the sixth register during a round of operation.

17. The apparatus of claim 12, wherein the second plurality of transformation units comprise a linear transformation unit coupling the fifth register to the fourth register to store a linearly transformed version of the content of the fifth register into the fourth register, factoring into consideration inputs from the first key section, during a round of operation.

18. The apparatus of claim 12, wherein the second plurality of transformation units comprise a linear transformation unit coupling the sixth register to the fifth register to store a linearly transformed version of the content of the sixth register into the fifth register, factoring into consideration inputs from the first key section, during a round of operation.

19. An apparatus comprising:

a first key section having a first, a second and a third register to be collectively initialized with a first cipher key, and a first plurality of transformation units coupled to the first, second and third registers to successively transform a selectively modified version of the first cipher key;

a data section having a fourth, a fifth, and a sixth register to be collectively initialized with a random number, and a second plurality of transformation units coupled to the second, fourth, fifth and sixth registers to successively and dependently, on the first key section, transform the random number;

a second key section coupled to the first key section to selectively modify the first cipher key; and

a mapping section coupled to the first key section and the data section to generate a pseudo random bit sequence.

20. The apparatus of claim 19, wherein the first plurality of transformation units comprise a plurality of substitution units coupled to the first and the third register to receive the stored content of the first register, make at least partial substitution to the received content and store the at least partially substituted content into the third register during a round of operation.

21. The apparatus of claim 19, wherein the first plurality of transformation units comprise a linear transformation unit coupling the second register to the first register to store a linearly transformed version of the content of the second register into the first register during a round of operation.

22. The apparatus of claim 19, wherein the first plurality of transformation units comprise a linear transformation unit coupling the third register to the second register to store a linearly transformed version of the content of the third register into the second register during a round of operation.

23. The apparatus of claim 19, wherein the second plurality of transformation units comprise a plurality of substitution units coupled to the first and the third register to receive the stored content of the first register, make at least partial substitution to the received content and store the at least partially substituted content into the third register during a round of operation.

24. The apparatus of claim 19, wherein the first plurality of transformation units comprise a linear transformation unit coupling the second register to the first register to store a linearly transformed version of the content of the second register into the

first register, taking into consideration inputs from the first key section, during a round of operation.

25. The apparatus of claim 19, wherein the first plurality of transformation units comprise a linear transformation unit coupling the third register to the second register to store a linearly transformed version of the content of the third register into the second register, taking into consideration inputs from the first key section, during a round of operation.

26. The apparatus of claim 19, wherein the second key section comprises one or more linear feedback shift registers (LFSRs) to output a first, a second and a third plurality of data bits; and a combiner function coupled to the LFSRs, and having a network of shuffle units serially coupled to each other, to combine the third plurality of data bits using the first and second plurality of data bits.

27. The apparatus of claim 19, wherein the mapping section comprises a plurality of logical gates coupled to the third and sixth registers of said first key and data sections respectively to generate said pseudo random bit sequence.